EXHIBIT C

UNCATEGORIZED

National Western Life Insurance company Nightmare Continues

By cybleinc
AUG 24, 2020

The number of cyberattacks in the insurance sector has been growing exponentially as insurance companies are migrating toward digital channels in an effort to expand their share of customer's financial portfolios. Although these digital investments provide new strategic capabilities, on the other side these innovations tend to introduce new cyber-risks and attack vectors to organizations that are relatively inexperienced at dealing with the challenges of an omnichannel environment.

On August 18, 2020, the Cyble Research Team during their daily monitoring of cyber threats and risks they identified a leak post in which the REvil ransomware operators claimed to have breached National Western Life and in possession of 656 GB of company's confidential data.

Founded in the year 1956, National Western Life is a well-known American stock life insurance company headquartered in Austin, Texas. With over 25000 employees the company has been earning annual revenue of around $636.2 million.

Snippet of the post on REvil website –

National western life
Headquarters:10801 N Mopac 3, Expy Bldg, Austin, Texas, 78759, United States
Phone:(512) 836-1010
Website:https://www.nationalwesternlife.com/
Stock Symbol:NWLI
We have 656 gigabytes of your confidential data. Folders: 25110 Files: 453695
Databases, contracts, projects, information about your clients and much more.
We gave you enough time to settle everything peacefully. But you have shown lack of discretion, apparently the confidentiality of your customers' data is an empty phrase for you.
We even have the passports of your children [redacted]

In that leak disclosure post, the ransomware group posted a couple of screenshots to support their claim of the breach which seems to include a snapshot of database files, passport copies of family members of the company's CEO, corporate contract agreements, information of their clients, and much more.

UNDERSTANDING CYBERSECURITY IN THE BANKING, FINANCIAL SERVICES AND INSURANCE (BFSI) IS AN INDUSTRY

EliteCISO Webina...
00:00 01:12:19

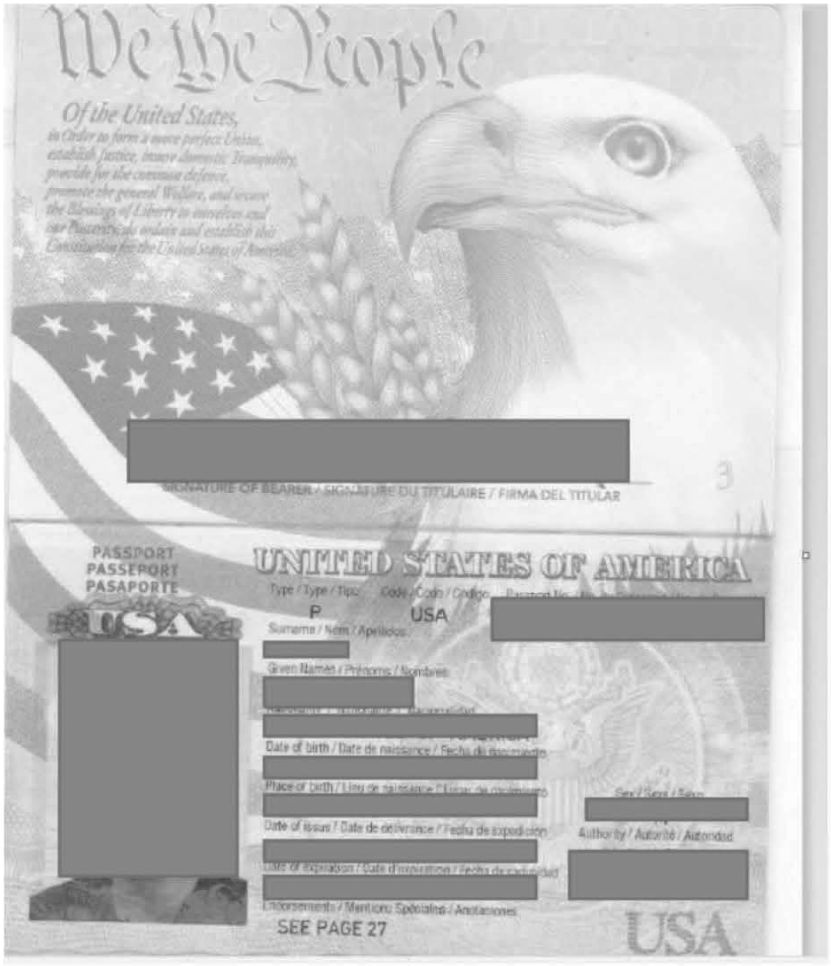
Search

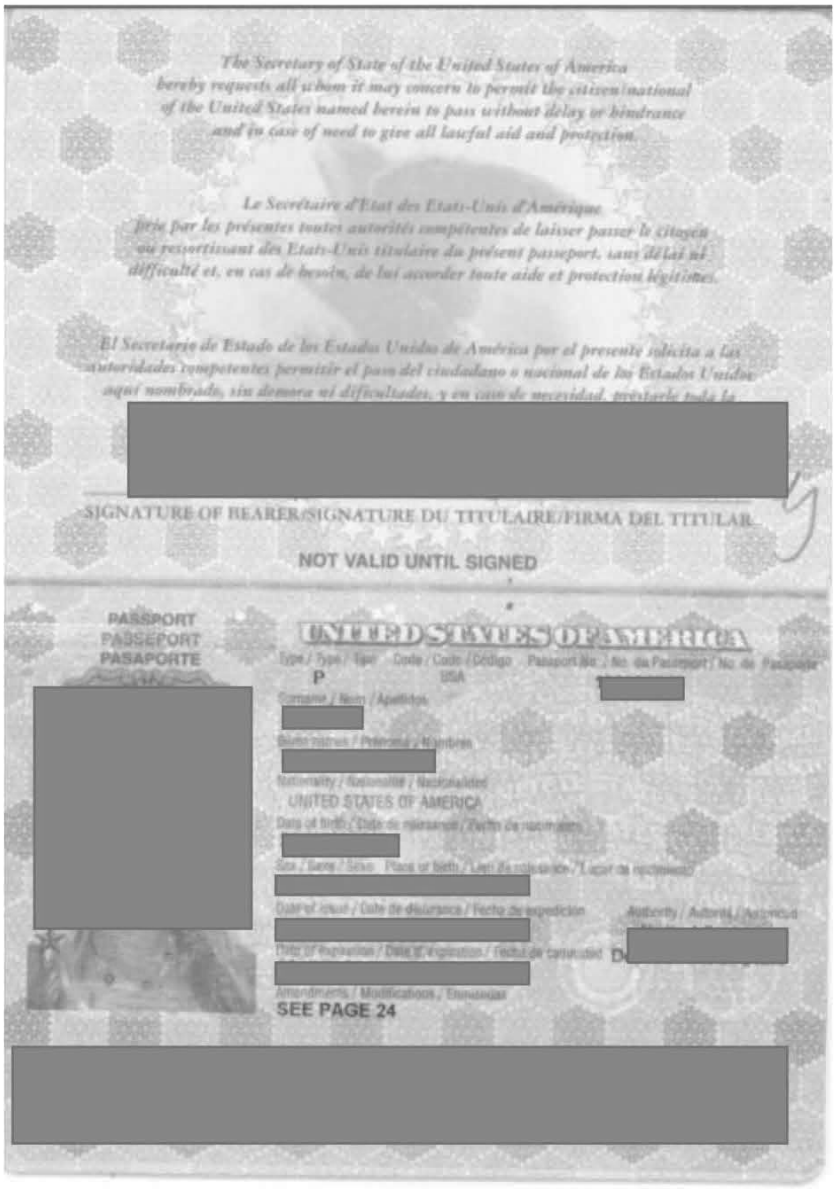
OUR BLOGS SCHEDULE

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

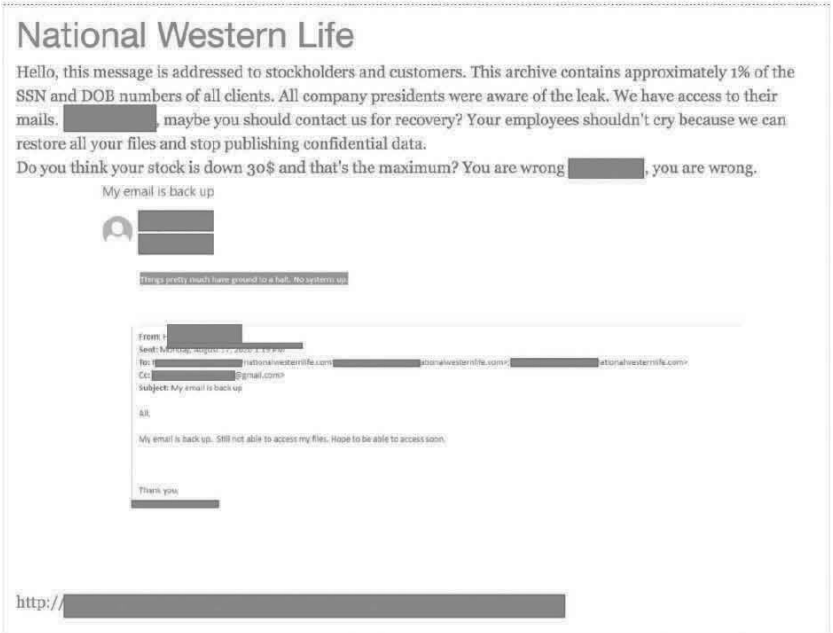
August 2020

awddb01.mdf	40gb
LifeCycleAccountHistory_Data.MDF	38gb
LifeCycle.MDF	24gb
LifeCycleBOD_Data.MDF	24gb
LifeCycleEOD_Data.MDF	24gb
LifeCycle_Pre02192014_Data.MDF	18gb
LifeCycle_Pre02272014_Data.MDF	14gb
AWDInput.mdf	11gb
Agency.mdf	5gb
LifeCycleArchive_Data.MDF	5gb
AgencyBOD.MDF	4gb
AgentDurationHistory.mdf	2gb
iWORKS.mdf	1gb
InsuranceSystem.mdf	1gb
LifeCycleDaily_Data.MDF	1gb
TMMonitor_Data.MDF	709mb
Claims.mdf	485mb
Contracts.mdf	412mb
Forms.mdf	331mb
LifeCycleIntegration.mdf	321mb
NWLAdmin.mdf	258mb
LifeCycleIntegration_log.ldf	146mb
AWDNba.mdf	108mb
NWLEMS.mdf	79mb
NBSupport.mdf	68mb
LifeCycleLapis.mdf	55mb
POSService.mdf	36mb
CaseManagement.mdf	15mb
CreditCard.mdf	14mb
iWORKS_DATATBL.ndf	10mb
iWORKS_OTHER.ndf	10mb
Complaints.mdf	6mb
Administration.MDF	5mb
SalesConference12.mdf	4mb
PlanCodeDerivation.mdf	3mb
InsuranceSystemIntegration.mdf	3mb
UPSWorldShip.mdf	3mb
AgentForms.mdf	2mb
LifeCycleSupport.mdf	2mb
Illustrationsdb.mdf	2mb





Then after 3 days on 23 August, the ransomware operators published another post in which they claimed to have access to the company's mails, and along with that they released 1% approx. of the total data leak. After analyzing the leaked files, it seems to contain details of the company's customers that include customer's SSNs, date of birth, full name, date of death, residence state, policy number, and policy termination date.



Below are the few snapshots of the leaked files being released by the REvil ransomware operators.

Tips on how to prevent ransomware attacks –

- Only download from sites you trust
- Never use unfamiliar USBs
- Use security software and keep it updated
- Backup your data periodically
- Isolate the infected system from the network
- Use mail server content scanning and filtering

It is recommended to follow above mentioned prevention methods and **never pay the ransom.**

***About** Cyble*

Cyble is an Atlanta, US-based, global premium cyber-security firm with tools and capabilities to provide near real-time cyber threat intelligence.

Cyble Inc.'s mission is to provide organizations with a real-time view of their supply chain cyber threats and risks. Their SaaS-based solution powered by machine learning and human analysis provides organizations' insights to cyber threats introduced by suppliers and enables them to respond to them faster and more efficiently.

This monitoring and notification platform gives the average consumer insights into their personal cybersecurity issues, allowing them to take action then as needed. It has recently earned accolades from Forbes as being the top 20 cyber-security companies to watch in 2020.

« One of the Giant Darkweb Markets Been Offline for Days

369K+ Alleged Banking records of Indian citizens Leaked on Darkweb »

By cybleinc

RELATED POST

Startup Cyble Raises Funding from Y Combinator

FEB 5, 2021

CYBLEINC

Cybercriminals Target Code Analytics Companies

FEB 2, 2021

CYBLEINC

Regains Its Foothold in the Threat Landscape

FEB 2, 2021

CYBLEINC

Leave a Reply

Your email address will not be published. Required fields are marked *